

Biztonság és védelem az informatikában

1. gyakorlati feladat

Készítette: Baranyi Gábor
CRC7FC

Források: <https://www.sans.org/newsletters/at-risk/>

Saját megfigyelések


2021.02.18

Operációs rendszerek biztonsága

Az operációs rendszerek szoftveres és hardveres elemei szempontjából is fontos, hogy megfelelő védelem alatt álljanak ne kerüljön információ illetéktelen emberek kezébe.


A SANS Security információbiztonságra, hálózatvédelemre, internetbiztonságra specializálódott szerv honlapján található heti összesítésben, hogy milyen biztonsági problémákat találtak az adott héten egy-egy operációs rendszeren, hálózati eszközön, vagy operációs rendszertől függetlenül futó alkalmazásnál.

Interested in a SANS course? Experience what a course is like by taking a free one hour demo of your choosing!

[Login](#) [Join Community](#)

[Train and Certify](#) [Manage Your Team](#) [Resources](#) [Focus Areas](#) [Get Involved](#) [About](#)

The most trusted source for cyber security training, certification, and research.




Introducing SANS Offensive Operations


Learn more about our brand new Offensive Operations Curriculum! The courses within this curriculum are broken up into different focus areas including:


- Penetration Testing
- Red Teaming
- Purple Teaming
- Exploit Development


[Learn More →](#)

1 2 3

[Find a Course](#) 

[Get Certified](#) 

[Earn a Degree](#) 

[Free Resources](#) 

Learn how SANS Institute is supporting the cyber security community during the COVID-19 Pandemic

[Read More →](#)

Training Options

OnDemand

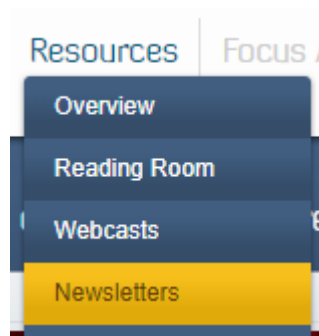
Four months of access

Flexible, self-paced training to fit your schedule including access to repeatable labs and quizzes, plus SME support.

Training Events


Live Streamed Instructor-Led

More than 60 SANS courses are delivered through our Live Online Training events, each across different global time zones to match your schedule.



A resources menüpontra kattintva és a newsletters menüpontot kiválasztva eljuthatunk erre az oldalra:

[Log In](#) [Join](#) [Contact Us](#) [SANS Sites](#) [Search](#)

 [Train and Certify](#) [Manage Your Team](#) [Resources](#) [Focus Areas](#) [Get Involved](#) [About](#)

[Home](#) > [Newsletters](#)

SANS Newsletters

SANS offers three newsletters to keep you up-to-date on the latest cybersecurity news, cyber attacks and vulnerabilities, and security awareness tips and stories. Subscribe below to gain access to these updates plus thousands of additional free SANS resources.

NewsBites

SANS NewsBites is an annotated, semiweekly executive summary of the most recent and important cybersecurity news headlines.

[→](#)

@RISK

@RISK provides a reliable weekly summary of newly discovered attack vectors, vulnerabilities with active new exploits, insightful explanations of how recent attacks worked, and other valuable data.

[→](#)

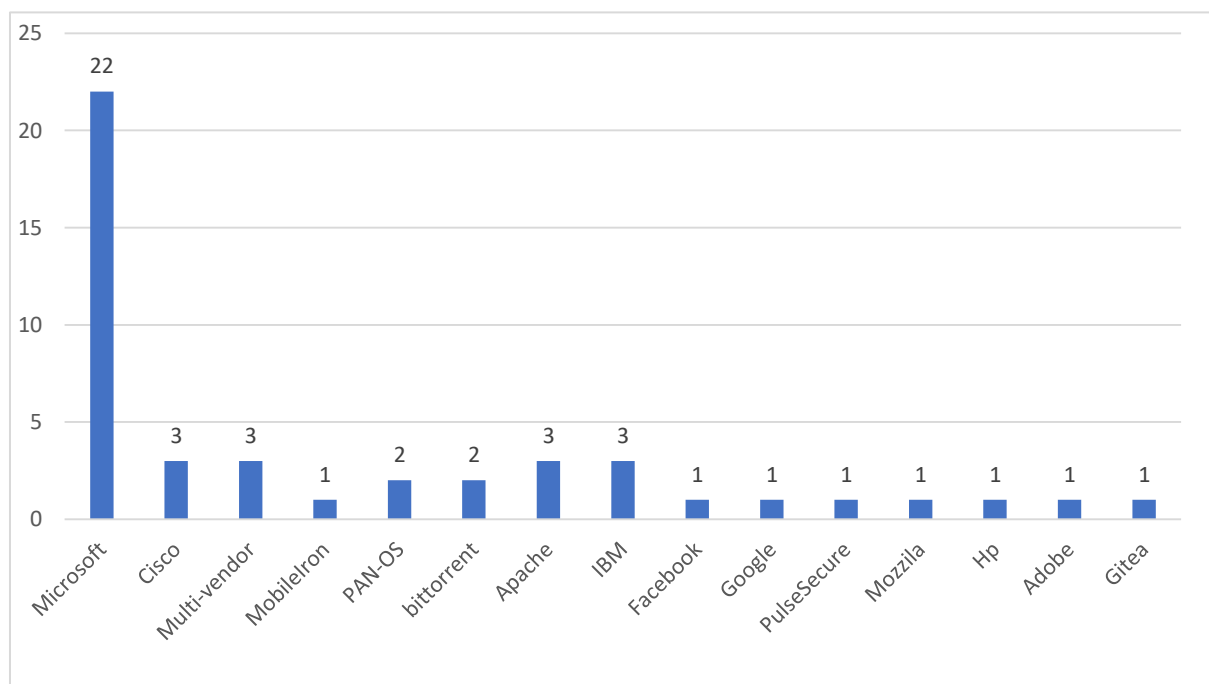
OUCH!

OUCH! is the world's leading, free security awareness newsletter designed for the common computer user.

[→](#)

Itt a @risk pontra kattintva megkapjuk sorozatban a heti összesítéseket, ahol kiválasztottam a 2020.09.17 – 2020.10.22 heteket, majd a feladat leírásnak megfelelően ki gyűjtöttem az adatokat a következő táblázatba.

	2020.09.17.	2020.09.24.	2020.10.01.	2020.10.08.	2020.10.15.	2020.10.22.
Microsoft	4	4	3	4	3	4
Cisco	0	0	1	1	1	0
Multi-vendor	2	1	0	0	0	0
MobileIron	1	0	0	0	0	0
PAN-OS	1	1	0	0	0	0
bittorrent	0	1	1	0	0	0
Apache	0	1	0	0	1	1
IBM	0	1	1	0	0	1
Facebook	0	0	1	0	0	0
Google	0	0	1	0	0	0
PulseSecure	0	0	0	1	0	0
Mozilla	0	0	0	1	0	0
Hp	0	0	0	0	1	0
Adobe	0	0	0	0	1	0
Gitea	0	0	0	0	0	1



A legtöbb hiba, mint a táblázat is mutatja a Microsoftnál merült fel. Az első négy vizsgált héten kivétel nélkül előfordult ezen Microsoft Exchange kiszolgálói hiba:

ID: CVE-2020-16875

Title: Microsoft Exchange Server Remote Code Execution Vulnerability

Vendor: Microsoft

Description: A remote code execution vulnerability exists in Microsoft Exchange server due to improper validation of cmdlet arguments. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the System user. Exploitation of the vulnerability requires an authenticated user in a certain Exchange role to be compromised.

CVSS v3 Base Score: 8.4 (AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:H)

Mely során egy részt kihasználva a támadó tetszőleges kódokat futtathat a támadott kiszolgálón.

További észrevételem még, hogy a problémák megoldása legtovább a Microsoftnál is tartanak, mert a Multi-vendor memória sebezhetősége két hét leforgása alatt lett kijavítva, de az újra indítási problémáját már a 2. vizsgálati hétre kijavították.

ID: CVE-2020-14386

Title: Linux kernel "af_packet.c" Memory Corruption Vulnerability

Vendor: Multi-Vendor

Description: A Memory corruption vulnerability exists in the Linux kernel that can be exploited to gain root privileges from unprivileged processes. The highest threat from this vulnerability is to data confidentiality and integrity.

CVSS v3 Base Score: 6.7 (AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H)

A legkevesebb hibát produkálók:

MobileIron

Facebook

Google

PulseSecure

Mozilla

Hp

Adobe

Gitea

Ők a hibájukat a következő hétre megszüntették, megoldották.